EXAMINATION BELIEF SENSING BASED PRIVACY PATH TECHNIQUE FOR WIRELESS SENSOR NETWORKS

R.PRADEEP RAJ
M.Tech Student, Dept. of CSE, Vaagdevi College of Engineering, Warangal, T.S

Dr.K. RAJESH KANNA
Assistant Professor, Dept. of CSE, Vaagdevi College of Engineering, Warangal, T.S

Abstract

Due to limited energy and poor deployment environments on database transmission, there is a serious impact on common network attacks, with a lightweight features and resistance capability, environment of Wireless Sensor Networks (WSNs). A trust-based secure routing mechanisms. (TSSRM) with lightweight features and the ability to resist many mutual attacks simultaneously This paper uses many common attacks at the same time, on the same time the security path selection algorithm is also enhanced by taking the confidence degree and core meter matrix accounts. Performance analysis and simulation results show that the TSSRM can improve the security and effectiveness of the WSNs.

Keywords*: Optimal Route Security, Wireless Sensor Networks, Quality of Service.*

I. INTRODUCTION

The rapid development of Internet of Things (IoT) promotes the continuous construction of cloud computing, social network and smart city. In various smart cities, wide variety of intelligent devices can provide wide-scale applications such as environmental monitoring, traffic management and social entertainment services. WSN played an important role in smart service services, with the features of low cost, rapid deployment and self-organization. Numerous sensors can gather the physical information of the citizens of Nodes and control public and private facilities in the context of a smart urban environment [1]. However, multi-road routing is dangerous for different types of attacks, due to the open, split and dynamic feature of WSN, which has a serious impact on data security and data. At present, the current secure routing algorithm is usually directed against specific abuses or automatic behavior attacks, because they primarily trust the encryption algorithms and authentication mechanisms, in which Multi-stop distribution and energy-based management are not suitable for WSN. Research shows that Trust Management (TM) is an effective way of solving security issues of WSN, however, to ensure that the traditional routing protocol can be trusted to ensure that multi-top information transfer the safety is difficult. , And can be summarized as reasons, although trust-based schemes can handle multiple attacks in WSN, they also promote some new risk. Second, the confidence is generally different from other general routes, hop, and delay or different from other QoS requirements, but do not consider the special asset of reliable degree in most credible model protocols. Third, the current routing is based on the current routing protocol, depending on the specific route scheme or platform. In other words, if the network routing protocol has been changed, the security method may be incorrect. This paper recommends a safe sensing based secure routing mechanism for WSN to solve network heading and transfer information about multiply information in this case [2]. And the results of the simulation show that the TSSRM also not only improves the impact of information for multi-touch communication networks but also its effects effectively. The main part of this

paper can be summarized as follows: 1) this sensor analyzes the behavior of nodes and sensor of energy sensor including nodes. The degree of sensor node is done according to these characters, and then the degree of trust is counted and the network calculation model is set, which means the source node is more than the destination node. . At the same time, the degree of trust and the QoS are combined as matrix routing to present the custom routing algorithm using semiconductor. 2) Safe routing mechanisms have been designed based on transmission, configuration and TSSRM working process has also been described. The analyzed routing algorithm applies to a safe routing mechanism so that the data is efficient and reliable transmission. At the same time, the maintenance of TSSRM is provided to ensure data transmission protection.This section analyzes several specific network attacks in WSN and uses its methods in a variety of ways in a variety of ways. According to different attacks on different attacks, attacks of protocol attacks and trust models can be stopped in joint attacks [3]. Multiple stop relay generally detects protocol attacks to avoid networking seriously. Generally, protocol attacks can be classified as soft attacks and tough attacks according to the behavior of router invaders. Soft attacks mean that unfortunately or self-determination nodes behavior cheats about cheating or fraudulent data. Such as: Black hole attack, which includes fake available channel information, on the way to the path, intentionally captures some data packets the sink attack, the Gray Hole The attack generates local resources. It is, the attack on wallet attack, which makes false lies by conspiracy, provides information while analyzing network traffic and forgets multi-identification of the attack on the cable. Trouble attacks mean that destroying existing transmission resources can harm transmission nodes, such as: Attacker's invaders [resources] attacker storm and bandwidth attacked the invaders unfortunately attacked. Even though the TM system handle more and more network attacks and can improve network security by encryption and TrustManagement, it is a new target of invaders. At this time, the general confidence model attacks include: attack attacks, attack on contradictory behavior, autonomous attack, bad mood attack and attack. In addition, the Trust Management algorithm, which can be widely used in encryption or transmission wireless communication network, is not suitable for all wireless networks, such as trust management algorithms [4].

II. LITERATURE SURVEY

This section analyzes many common network attacks Extends WSN and their role to help them The purpose of WSN's security assistance after network attacks Various items using different modes. General attacks can be divided into protocols Attacks and confidence model attacks according to different attacks Goals target multi-stop relays to protocol routing Attack against more than double wireless attacks Communications network routing, protocol attacks routine According to this, soft attacks and severe attacks can be classified Invaders' behavior. Soft attacks mean that unfortunately Or destroy stolen nodes behavior by stealing or storing data Or cheats cheating such as: black hole attack Adds false available channel information to the application of routing, The Gray Hole attack which deliberately stops some data packets [5], attack on sinkhole, which generates local resources Attack on the attack on which false links

are built by the conspiracy Information is detected by analyzing network traffic, At the same time, Apple's attack has also forgotten multi-identity [6]. Hard the attacks mean that unfortunately nodes damage the information By transmission of existing transmission resources, transmission, As such: the DOS attack on which the attacking resources have been removedThings Attack on Bollywood which captures bandwidth unfortunately. Although the TM system can handle the network most of the time Improve network security through attacks and encryption and trust mechanism, perhaps it becomes a new target Invaders at this time, common trust model attacks include: Attack, counter attack, autonomous attack, Bad Mouth Melt and Assault Attack. Other than that, The Trans Management Algorithm that accepts encryption or trust there are widely used mechanisms in the wireless communication network Because of the trust, not all wireless networks are suitable for The Management Algorithm focuses on the reliability process and ignores the confidence-driven process. In fact, to Confidence of confidentiality, ensuring the accuracy of the trust frequently based on confidence, which leads to someone large quantity of head [7], TM is difficult to apply directly managed WSN. Therefore, light weight Security routing mechanisms in this paper will be constructed the degree of trust and energy by energy, and together TSSRM with lower value QoS to design the Metrics designmany types of common attacks can compete.

III. A TRUST SENSING BASED SECURE ROUTING MECHANISM

A trust sensing based secure routing mechanism (TSSRM)is proposed according to the constructed routing metrics and the optimal credible route selection algorithm.

This paper analyzes the behavior of sensor nodes Sensor nodes movement and energy consumption. The degree of sensor node is done according to them the letters, and then the trust degree count is counted And network trust calculator model has been established Get the most out of the source node floor Node. At the same time, the degree of confidence and the square meter Routing Matrix is a custom to present Using algorithms to prevent the algorithms. Trans-transaction mechanism based on trans-sensing Design, Testing and TSSRM are the working processes .This paper is also described. Recommended routing algorithms secure routing mechanisms are applied to the mechanism Data efficient and reliable transmission. At the same time, The TSSRM maintenance process has also been presented Ensure data transmission protection [8].

Trust degree is an important foundation for assessing confidence the relationship is adopted in Analytic hierarchy process (AHP) Analysis and confidence of this section to analyze the model. The whole multi-way path is the calculation model two nodes (including direct trust degree, indirect trust degree and motivation element) decide a secure way of transmission of data.

Direct Trust Calculation of Nodes:

Attitude of Sensor Nodes may be monitored by the neighbor nodes in WSN. Since Sensor Nodes are limited to the extremely computing power, Energy, memory and bandwidth, it's not enough to decide Nodes trust only by monitoring nodes Therefore, this study will combine energy behavior

comprehensively.Discover the confidence of nodes [9].

Nodes will choose with high confidence in the network The degree as a relay to promote information traditionally Security model, which is to increase energy consumption Nodes with advanced degrees, consequently unusual result Network load or even network distribution. Therefore, According to the calculations, the model module will include energy reliability Node Y's energy consumption indicates trust degree the message is shown during receiving and sending (3) and (4) respectively [10].

CLUSTER HEAD SELECTION ARCHITECUTE:

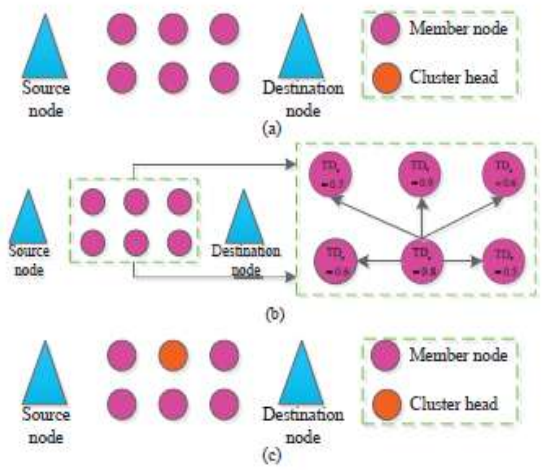

Fig.1 Cluster Head Selection

This paper will choose nodes with high initial confidence Degree as Cluster Head. Higher Node Trust Degree its energy is high, and long-term nodes are lifetime, which is more favorable for the stability of the cluster structure. Cluster head selection process of clustering topology The 6 nodes contained in the model Fig.1.

Trust model based on AHP

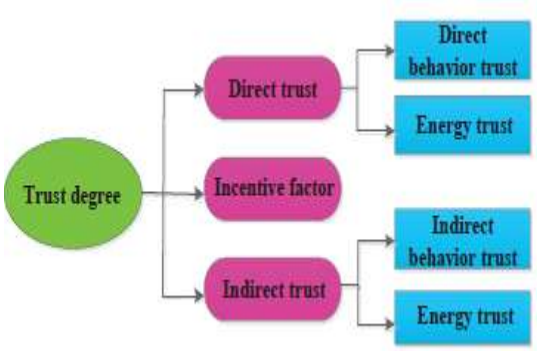

Fig.2 Trust model based on AHP

Analytic hierarchy process (AHP) is adopted in this paper to establish a comprehensive trust model, which is based on direct trust, indirect trust and incentive factor, as shown in Fig.2.

IV. CONLCUSION:

WSN is an important part of the modern communication system, and trust the sensing routing protocol for WSN Effective way to improve security, therefore, studying trust Sensing routing protocol is very important. This paper offers To handle a trusted sensing based secure routing mechanism Combined network attacks have a custom routing algorithm Recommended using a semiring principle, which considers trust Degree and other QoS Metrics. Simulation results show that The TSSRM can reduce the RM road and reduce it traditionally reliability of data transmission Trust mechanism. Future research will be distributed Intervention Detection System for WSN, which can provide a new one the way to trust the degree and the appropriate route research

V. REFERENCES

[1] N. Marlon, C. Jose, A. B. Campelo, O. Rafael, V. C. Juan, and J. S. Juan, "Active low intrusion hybrid monitor for wireless sensor networks," Sensors, vol. 15, no. 3, pp. 23927-23952, 2015.

[2] G. Ottman, A. Bhatt, H. Hofmann, and G. Lesieutre, "Adaptive piezoelectric energy harvesting circuit for wireless, remote power supply," IEEE Transactions on Power Electronics, vol. 17, no. 5, pp. 669-676, Sep. 2002.

[3] W. K. K. Chin, and K. L. AYau, "Trust and reputation scheme for clustering in cognitive radio networks," International Conference on Frontiers of Communications, Networks and Applications (ICFCNA), KualaLumpur, Malaysia, Nov. 2014, pp. 1-6.

[4] Y. Gao, H. W. Chris, J. J. Duan, and J. R. Chou, "A novel energyaware distributed clustering algorithm for heterogeneous wireless sensor networks in the mobile environment," Sensors, vol. 15, no. 10, pp. 31108- 31124, 2015.

[5] J. P. Yao, S. L. Feng, X. Y. Zhou and Y. Liu, "Secure routing in multi-hop wireless ad-Hoc networks with decode-and-forward relaying," IEEE Transactions on Communications, vol. 64, no. 13, pp. 753-764, 2016.

[6] P. Balasubramanian, J. V. P. Maria, K. Madasamy, "Development of a secure routing protocol using game theory model in mobile ad hoc networks," Journal of Communications and Networks, vol. 17, no. 13, pp. 75-83, 2015.

[7] J. Cordasco, and S. Wetzel, "Cryptographic versus trust-based methods for MANET routing security," Electronic Notes in Theoretical Computer Science, vol. 197, no. 2, pp. 131-140, 2008.

[8] A. Cornejo, S. Viqar, and J. L. Welch, "Reliable neighbor discovery for mobile ad hoc networks," Ad Hoc Network, vol. 12, no. 6, pp. 259-277, 2014.

[9] Y. Sun, Z. Han, and K. J. R. Liu, "Defense of trust management vulnerabilities in distributed networks," IEEE Journals and Magazines, vol. 46, no. 2, pp. 112-119, 2008

[10] P. F. Xu, Z. G. Chen, and X. H. Deng, "Research on neighboring graphs based topology control in wireless sensor networks," Electronic Industry Press, Beijing, pp. 13-17, 2006.